a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #13
Securing User Accounts

Introduction

1. User Accounts control access to UBC Electronic Information and Systems and as such they must be effectively protected against unauthorized access. This standard is closely tied to the User Account Management standard.
2. This document defines standards that University IT Support Staff must comply with when securing these accounts.
3. The Chief Information Officer has issued this document under the authority of Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

Password Protection Requirements

4. All User Accounts must be password protected in accordance with the Password and Passphrase Protection standard. Where possible, systems should enforce password complexity rules in accordance with that standard.
5. Users who receive new accounts or who require a replacement password must be provided with a temporary password, which is forced to change upon first login. Temporary passwords must be given to Users in a secure manner.
6. Procedures must be established to verify the identity of a User prior to providing a new, replacement or temporary password for an account. It is recommended that identification procedures follow the standard practice of validating the answers to three questions that were previously created by the User during account creation (this procedure is mandatory for CWL password changes).
7. Default vendor passwords must be changed following the installation of systems or software.

Authentication System Requirements

8. Where possible, all User Accounts should be centrally controlled in the UBC Enterprise Active Directory, Enterprise LDAP, or Campus-Wide Login.
9. Authentication systems for User Accounts must be adequately protected from password cracking using at least one of the following methods:
    a. the account is locked for a period of time if an incorrect number of passwords/passphrases is entered over a specified time period (for example, if an incorrect password/passphrase is entered 10 times within a 30 minute window, the account will be locked for 30 minutes); and/or
    b. each time an incorrect password/passphrase is entered, the system introduces a delay before providing the failure response; this delay increases as the failed login attempts continue but will reset once the User successfully logs in (for example, the delay period could begin at 100 milliseconds, and double after each subsequent failed login).
10. Authentication systems must not store account passwords in clear text. Where possible, passwords should be stored using a strong cryptographic hash and salted; for further guidance see Salted Password Hashing - Doing it Right.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Password and Passphrase Protection standard

User Account Management standard